



## DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

(51) Classification internationale des brevets <sup>7</sup> : <b>H04Q 7/38</b>	<b>A1</b>	(11) Numéro de publication internationale: <b>WO 00/25546</b> (43) Date de publication internationale: 4 mai 2000 (04.05.00)
---	-----------	---

(21) Numéro de la demande internationale: PCT/FR99/02233

(22) Date de dépôt international: 21 septembre 1999 (21.09.99)

(30) Données relatives à la priorité:  
98/13440 27 octobre 1998 (27.10.98) FR

(71) Déposant (pour tous les Etats désignés sauf US): GEM-PLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F-13881 Gémenos Cedex (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (US seulement): LE GALL, Jean, Pierre [FR/FR]; Chemin Saint Marc, F-13790 Rousset (FR).  
CHEW, Gary [SG/FR]; 397 Rue Paradis, F-13008 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Parc d'Activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.

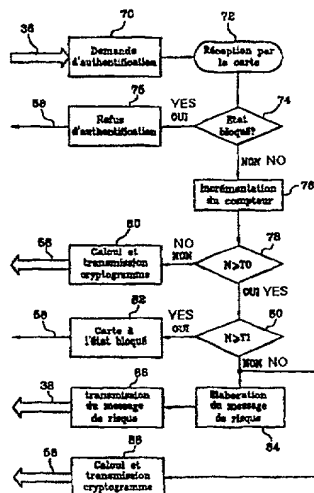
(54) Title: MOBILE METHOD AND SYSTEM FOR MANAGING RISK IN A MOBILE TELEPHONE NETWORK.(54) Titre: PROCEDE ET SYSTEME DE GESTION DU RISQUE DANS UN RESEAU DE TELEPHONIE MOBILE

## (57) Abstract

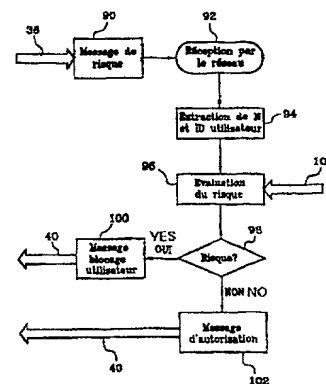
The invention concerns mobile telephone system networks, characterised in that the electronic chip card (22, SIM) comprises means (32) for authorising or not the computation of a cryptographic certificate and transmitting (56) it to the network when certain conditions are fulfilled or not and for transmitting to the network a message (38) requesting to assess risk when other conditions are fulfilled. Moreover, the network (54) comprises means (34) for assessing said risk on the basis of data contained in the message (38) requesting assessment of the risk and user-specific parameters and for sending a message (40) to said means (32) authorising or not the computation and transmission of the cryptographic certificate.

## (57) Abrégé

L'invention concerne les réseaux de téléphonie mobile. L'invention réside dans le fait que la carte à puce électronique (22, SIM) comprend des moyens (32) pour autoriser ou non le calcul d'un certificat cryptographique et sa transmission (56) au réseau lorsque certaines conditions sont remplies ou non et pour transmettre au réseau un message (38) de demande d'évaluation du risque lorsque d'autres conditions sont remplies. Par ailleurs, le réseau (54) comprend des moyens (34) pour évaluer ledit risque en fonction des informations contenues dans le message (38) de demande d'évaluation du risque et de paramètres spécifiques à l'utilisateur et pour envoyer un message (40) auxdits moyens (32) pour autoriser ou non le calcul et la transmission du certificat cryptographique.



70...REQUESTING AUTHENTICATION  
72...RECEPTION BY CARD  
74...OFF STATE ?  
75...AUTHENTICATION DENIED  
76...INCREMENTING COUNTER  
80...COMPUTING AND TRANSMITTING CRYPTOGRAM  
82...CARD IN OFF STATE  
84...PREPARING RISK MESSAGE  
86...TRANSMITTING RISK MESSAGE  
88...COMPUTING AND TRANSMITTING CRYPTOGRAM



90...RISK MESSAGE  
92...RECEPTION BY NETWORK  
94...EXTRACTING N AND USER ID.  
96...ASSESSING RISK  
98...RISK ?  
100...MESSAGE FOR BLOCKING USER  
102...AUTHORISATION MESSAGE